DRAFT

REMARKS/ARGUMENTS

I. Introduction

Applicant thanks the examiner for continuing examination.

- Claims 79-117 remain in this application.
- Claims 79 and 99 are the only independent claims under review.
- Claims 79-82, 89, 97-100, 103, 112, 113, 115-117 stand rejected under 35 U.S.C. § 102(e).
- Claims 83-88, 90-96, 101, 102, 104-108, 109-111 and 114 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over **Shi** et al., US pat. No. 5,875,296 in view of **Wiser** et al., US pat. No. 6,385,596.[1]
- **White**, US pat. No. 6,049,877, prior art made of record and not relied upon, is considered pertinent to applicant's disclosure.

II. Claims

A. Rejections under 35 USC § 102(e) are improper.

1. The rejection to Independent Claim 79 is improper because **Shi** does not teach "secure cookies."

First, **Shi** does not teach "secure cookies." Rather, **Shi** discloses the use of a persistent client state HTTP cookie authentication scheme as part of authenticating users who access a distributed file system through an Internet World Wide Web server. See **Shi**, col. 2, lines 26-49. This scheme introduces a cookie to the client by including a Set-Cookie header as part of an HTTP response, such as a CGI script, through a server-side connection. Id. at col. 6, lines 48-63. **Shi** indicates that if a cookie is marked "secure," then the cookie will only be transmitted if there is a secure communications channel with the host. Id. at col. 7, lines 64-67. Otherwise, if "secure" is not specified, then a cookie may be considered to be safely transmittable over unsecured channels. Id. at col. 8, lines 1-3.

However, this unencrypted variable called "secure" discloses a conventional cookie because the word "secure" in **Shi** refers to the security level of a communications channel. This necessarily means that conventional cookies as used in **Shi** provide no security other than a secure network connection through both an initial user id and password,

[1] Examiner makes no explanation how claims 90-95, 105-107, and 109-110 are rejected under 35 U.S.C. § 103(a) as being unpatentable over **Shi** in view of **Wiser**. Rather, examiner only states that **Shi** discloses these claims in his rejection. Applicant would appreciate clarification on how these claims are obvious over **Shi** in view of **Wiser**.

and a later created unique id. This lack of security is exactly the problem that the present application, as disclosed and claimed, solves. See Specification, § 3.5 (stating that regular cookies (i.e., conventional cookies) "cannot protect cookies from the end-system threats").

Second, unlike the present application, **Shi** fails to teach how cookies may be secured. The present application relates to methods and devices for making "secure cookies" and specifically defines that "[s]ecure cookies are constructed by using familiar cryptographic techniques, such as message digests, digital signatures, message authentication codes and secret-key encryption." See Specification, p. 2, ¶ 2. How a secure cookie is generated depends on the circumstances. See, e.g., Specification, § 3.1 (stating that choosing an authentication cookie depends on the situation). "The novelty lies in the manner in which these techniques are applied to implement secure cookies and in the Web services to which secure cookies are applied." See Specification, p. 2, ¶ 2. For instance, as one notable aspect, one Web server may issue secure cookies for another client's use. Id. In contrast, **Shi** only exercises a method of using both an initial user id and password, and later created unique id for authenticating a user. Although the present application does teach a message authentication code based on a password, this technique does not require both a user id and password. Instead, only the hash of a password or an encrypted password is necessary. See Specification, § 3.1.2. Furthermore, **Shi** does not teach the above-exemplified notable aspect. Hence, the present application uniquely provides novel features that **Shi** fails to teach.

Third, the present application notes that security concerns pose security threats to regular cookies. See Specification, §§ 2.2-2.3. Particularly, these sections describe how regular cookies are susceptible to alteration and copying. The ability to copy cookies facilitates forgery and impersonation of an authenticated user, as well as enables an attacker to harvest cookies and employ such harvested cookies against a user. A mere simple secure network connection, by itself, does not provide sufficient protection. Id. at § 2.4.

Curbing these criminal acts, the present application teaches how secure cookies may provide authentication services, integrity services and confidentiality services. See Specification, § 3. "Authentication services verify the owner of the cookies." Id. "Integrity services protect against the threat that the contents of the cookies might be changed by unauthorized modification." Id. "Confidentiality services protect against the values of the cookies being revealed to unauthorized entry." Id. A careful read of **Shi** clearly shows that none of these services are either defined or taught in **Shi**.

Because **Shi** fails to teach the "secure cookies" limitation of independent claim 79, **Shi** does not disclose the same invention. Therefore, withdrawal of this rejection is respectfully requested.

2. The rejection of Claim 81 is improper because **Shi** does not teach an "authentication cookie."

Shi does not teach an "authentication cookie." An authentication cookie is defined in the present application on page 12, last paragraph, as an IP Cookie, a Pswd Cookie, a KT Cookie or a Sign Cookie. An IP cookie (address-based authentication) is created when a server grabs the user's IP address and puts it into the IP Cookie using internal procedures. See Specification, § 3.1.1. A Pswd Cookie (password-based authentication) is created when a server places a user's password and puts it into the IP Cookie using internal procedures such as a hash or encryption. Id. at § 3.1.2. A KT Cookie (Kerberos-based authentication) is created when a server creates a cookie that can be used in a Kerberos protocol. Id. at § 3.1.3. A Sign Cookie (digital-signature-based authentication) uses a timestamp signed by a user. Id. at § 3.1.4.

In making this rejection, the examiner brings attention to col. 5, line 24 to col. 6, line 67 of **Shi**. **Shi** teaches "it is desirable to enable a user of the client machine (intentionally or unknowingly) to use the (preferably) off-the-shelf browser to access, browse and retrieve documents located in the distributed file system." See **Shi**, col. 5, lines 26-29. **Shi** exemplifies such system with Distributed File Services (DFS), which is a known to be implemented in a networked environment called the Distributed Computing Environment (DCE). Id. at col. 5, lines 30-33. A person of ordinary skill in the art would know that DFS uses DCE Kerberos-based authentication. Id. at col. 5, lines 61-62. However, **Shi** dispels the notion of using the basic authentication scheme. In its place, **Shi** specifically uses "Persistent Client State HTTP cookies." Id. at col. 6, lines 49-50. Nowhere in this section is a "Persistent Client State HTTP cookie" the same as or equivalent to an authentication cookie (i.e., an IP Cookie, a Pswd Cookie, a KT Cookie, or a Sign Cookie). Rather, a "Persistent Client State HTTP cookie" is introduced to a client, usually through server-side connections (e.g., CGI script) by including a Set-Cookie as part of an HTTP response, for storing and retrieving information. Id. at col. 6, lines 51-63.

With respect to a Pswd Cookie (password-based authentication), **Shi** discloses an entirely different method. As discussed in section II.A.1., **Shi** only exercises a method of initially using both a user id and password, which are later replaced with a unique id created by the server for

authenticating a user. See **Shi**, col. 8, line 14 – col. 9, line 21. Compared to **Shi**, the password authentication method in the present application does not require both a user id and password. Instead, only the hash of a password or an encrypted password is necessary. See Specification, § 3.1.2. Therefore, **Shi** does not disclose what the present application teaches.

In addition, **Shi** discloses the use of DCE Kerberos-based authentication in a DFS that specifically requires different components. **Shi** requires a unix "credential," which is a data structure defining a particular machine by associating itself with each file operation while holding local authentication information within each file operation. This credential includes "a user id, a group id, optionally a list of operating system privileges, and an authentication identifier known as a PAG (Process Authentication Group)." Id. at col. 5, line 67 – col. 6, line 2. PAG "acts as a tag for associating 'tickets' between DFS and the DCE Security Server." Id. at col. 6, lines 3-4.

However, the Kerberos-based authentication cookie in the present application does not operate with a unix credential that uses "a user id, a group id, optionally a list of operating system privileges and an authentication identifier known as PAG." Rather, Kerberos-based authentication cookies in the present application require "an additional browser software to replace the value of the cookie (TGT_Cookie), which is containing a ticket-granting ticket (TGT)," and needs authenticators ({timestamp} S_A, {timestamp} $K_{C,S}$) to be generated in the TSK_Cookie and TSS_Cookie respectively. See Specification, § 3.1.3. Because of these significant differences, **Shi** could not anticipate the present application.

Lastly, there is no disclosure anywhere in **Shi** that references an IP Cookie (address-based authentication) or a Sign Cookie (digital-signature-based authentication).

Because **Shi** fails to teach the "authentication cookies" limitations of Claim 81, withdrawal of this rejection is respectfully solicited.

3. The rejection of Claim 82 is improper because **Shi** does not disclose a "secure attribute service."

Claim 82 further limits the "secure attribute service." **Shi** does not disclose a secure attribute service as defined in the present application. In the present application, "secure cookies enable secure attribute services between existing Web servers and browsers." See Specification, p. 2, ¶ 2. It is this use of secure cookies that "facilitates secure attribute services on

the Web." Id. Because **Shi** does not disclose "secure cookies" as argued in section II.A.1. above, **Shi** cannot disclose a "secure attribute service."

Because **Shi** fails to disclose the "secure attribute service" limitations of Claim 79, withdrawal of this rejection is respectfully solicited.

4. The rejection of Claims 89, 103, 112 and 115 is improper because **Shi** does not disclose the same requirements of a Kerberos–based authentication cookie as that of the present application.

In support of the rejection, the examiner cites col. 5, line 40 to col. 6, line 12; col. 1, line 51 to col. 2, line 18; col. 5, line 39 to col. 6, line 67 and col. 7, line 15 to col. 8, line 61. However, as previously discussed above in section II.A.2., a Kerberos-based authentication method in **Shi** is significantly different from the present application. **Shi** requires a combination of "a user id, a group id, optionally a list of operating system privileges, and an authentication identifier known as a PAG (Process Authentication Group)." Id. at col. 5, line 67 – col. 6, line 2. Quite the contrary, the present application requires "additional browser software to replace the value of the cookie (TGT_Cookie), which is containing a ticket-granting ticket (TGT)," and needs authenticators ({timestamp} S_A, {timestamp} $K_{C,S}$) to be generated in the TSK_Cookie and TSS_Cookie respectively. See Specification, § 3.1.3.

Because **Shi**'s requirements in a Kerberos-based authentication method differ from the present application's requirements, withdrawal of these rejections is respectfully requested.

5. The rejection of Claims 97, 98, and 116 is improper because **Shi** does not disclose any "secure cookies" used in electronic transactions or used to assign client roles.

The examiner refers to figs. 1; 2; abstract; col. 4, line 9 to col. 5, line 60 and col. 6, lines 2-47. However, nowhere does **Shi** disclose any "secure cookies" for electronic transactions (e.g., financial transactions). Furthermore, a careful read of these figures and paragraphs only illustrate the basic system of authenticating a user, whereby a path check checks whether the user has appropriate DCE credentials after a user requests a DFS document, that is used by a conventional (i.e., not secure) cookie. Upon proper authentication, **Shi** permits the user to retrieve requested documents. Moreover, **Shi** is not assigning a role as per the present application, but having a server assign an identifier to a process whose role has already been defined by a previous, successful login.

In contrast, the present application applies secures cookies in electronic transactions and a role-based access control (RBAC) in assigning client roles. See Specification, §§ 4.2, 4.4. Regarding electronic commerce, secure cookies in the present application make it unnecessary to have a customer-information database, which stores customers' access histories and sensitive information (e.g., credit card numbers and addresses), unless the site needs to tack such information. Id. at § 4.2.

With respect to assigning client roles, RBAC, an alternative to traditional discretionary and access controls, supports data abstraction, least-privilege assignment and separation of duties. See Specification, § 4.4. "With RBAC, system administrators can create roles, grant permissions to those roles, and then assign users to the roles on the basis of their specific job responsibilities and policy." Id.

Because **Shi** does not disclose any "secure cookies" used in electronic transactions or used to assign client roles, withdrawal of these rejections is respectfully solicited.

6. The rejection of Claim 99 is improper because **Shi** does not disclose "secure cookies" in the steps as specifically laid out in the claim.

Shi does not disclose the use of "secure cookies" in any of its steps. The examiner appears to concede that **Shi** does not use a "secure cookie." The examiner argues that figs. 1; 2; abstract; col. 4, line 9 to col. 5, line 60 and col. 6, lines 2-47 of **Shi** demonstrate the server as "processing data upon receiving request from a client and creating a cookie according to credentials of a user." By mentioning the word "cookie" without expressly using the word "secure," the examiner concedes that **Shi**'s cookie is a regular or conventional cookie. Alternatively, regardless of whether the examiner intended to leave out the word "secure," **Shi** still does not create in any step a "secure cookie" as defined within the scope of the present application. See Specification, p. 2, ¶ 2; §§ 3-3.5 (discussing various means of creating secure cookies and comparing regular cookies with secure cookies); supra § II.A.1.

In addition, the examiner has not shown the steps as laid out in claim 99. For each particular step, the examiner has referred to independent paragraphs or figures in **Shi**. For example, the examiner pieces together fig. 1 and col. 4, lines 8-48 of **Shi** to show a server retrieving conforming client data in response to the client request. This section of **Shi** only describes possible hardware and software that may be used in the **Shi** invention. There are no steps recited here. This rejection continues in this same manner.

In summary, because **Shi** does not disclose the steps of the present application, **Shi** does not disclose the invention claimed in claim 99. Therefore, withdrawal of this rejection is respectfully solicited.

7. The rejection of claims 80, and 100, 113 and 117 are improper because they depend upon independent claims 79 and 99 respectively.

The Office Action does not establish a prima facie case of anticipation of claims 80, 100, 113 or 117. Based upon the previous arguments, it is believed that independent claims 79 and 99 are now in condition for allowance. Claims 80, and 100, 113 and 117 depend on claims 79 and 99 respectively, and hence contain all of the limitations of their base claims. Therefore, withdrawal of these rejections is respectfully solicited.

B. Rejections under 35 USC § 103 are improper.

1. The rejection of Claims 83-88, 90-96, 101, 102, 104-108, 109-111 and 114 under 35 U.S.C. § 103(a) as being unpatentable over **Shi** in view of **Wiser** are improper because they all depend upon independent claims 79 and 99.

"All words in a claim must be considered in judging the patentability of that claim against the prior art." In re Wilson, 424 F.2d 1382, 1385, 165 USPQ 494, 496 (CCPA 1970); MPEP § 2143.03. "If an independent claim is nonobvious under 35 U.S.C. 103, then any claim depending therefrom is nonobvious." In re Fine, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988). Because claims 83–88 and 90–96 ultimately depend upon independent claim 79 and claims 101, 102, 104-108, 109-111 and 114 ultimately depend upon independent claim 99, the rejections of all of these claims are improper.

Furthermore, Applicant believes that the arguments previously made in section II.A. equally apply to the examiner's 35 U.S.C. § 103(a) rejections. These arguments overcome the rejections to independent claims 79 and 99 respectfully. Therefore, withdrawal of these rejections is respectfully solicited.

2. The rejection of claims 83-88, 90-96, 101, 102, 104-108, 109-111 and 114 under 35 U.S.C. § 103(a) as being unpatentable over **Shi** in view of **Wiser** are improper because it appears that the examiner has failed to make a prima facie case of obviousness.

Bearing the initial burden, the examiner seems to have not made a prima facie case of obviousness. The three elements that must be satisfied are:

> First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations.

MPEP § 2143.

Relying on **Shi** in view of **Wiser**,[2] the examiner concedes that "**Shi** does not specifically disclose the client's IP address, a hashing algorithm, and a digital signature on a timestamp, secret-key based authentication service." See Off. Action at 6-7, Nov. 19, 2003. However, the examiner points out that **Wiser** does. Id. Yet, nonetheless, there appears to be a lack of any suggestion or motivation to modify or combine these references to properly deny the present application a patent. Both **Shi** and **Wiser** are different inventions when compared to the present application. On one hand, **Shi** identifies a method of authenticating a user on a distributed file system through the use of cookies. See **Shi**, Abstract. On the other hand, **Wiser** addresses a computer implemented online music distribution system for secure delivery of media files for use on predetermined media players. See **Wiser**, Abstract. Simply, one of ordinary skill in the art may find it obvious to combine the two against an application that provides a method of using cookies to authenticate users who seek secure delivery of audio data. However, when viewed in their entirety, neither **Shi** nor **Wiser** address, allude to or provide the slightest notion for creating and using an independent secure cookie between a client and a server. From another perspective, **Shi** and **Wiser** provide one level of securing personal data, whereas the present application provides a

---

[2] The examiner relies on **Shi** and **Wiser** for an obviousness rejection, but incorrectly combines **Angles** into his explanation. See Off. Action at 7, Nov. 19, 2003 (stating that

> it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement **Wiser's** teachings into the computer system of **Angles** to identify a host computer because it would have enabled users to identify a host connected to the Internet to other Internet hosts and provided more secure delivery of data over the Internet.).

Applicant respectfully notes that examiner is repeating arguments made from the May 28, 2003 Office Action.

different level of securing personal data. Hence, there cannot be any suggestion or motivation to modify or combine **Shi** and **Wiser**.

Alternatively, even if the examiner is correct that such suggestion or motivation exists, the combined prior art do not teach all the claim limitations. Neither **Shi** nor **Wiser** disclose how to create or use an independent secure cookie. Rather, **Shi** and **Wiser** merely identifies other means of protecting personal data over communication networks. It is important to note that the Federal Circuit held that the teaching or suggestion to make the claimed combination must be found in the prior art but not in the present application's disclosure. In re Vaeck, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991). Because the **Shi** and **Wiser** combination does not teach or suggest how to create or use an independent secure cookie, the examiner erred in making an obviousness rejection.

Based on the lack of a prima facie case of obviousness, withdrawal of the obviousness rejection is respectfully requested.

3. Alternatively, the rejection of claims 83-88, 90-96, 101, 102, 104-108, 109-111 and 114 under 35 U.S.C. § 103(a) as being unpatentable over **Shi** in view of **Wiser** are improper because they appear to be based on impermissible hindsight.

Obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. In re Jones, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992); In re Fine, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988). See also MPEP § 2143.01. It should be recognized that prior art could be modified so as to result in the combination defined by the claims at bar would not have made the modification obvious unless the prior art suggests the desirability of the modification. In re Deminski, 796 F.2d 436, 230 USPQ 313 (Fed. Cir. 1986). Recognizing that such a modification would provide an improvement or advantage, without suggestion thereof by the prior art, rather than dictating a conclusion of obviousness, is an indication of improper application of hindsight considerations. Simplicity and hindsight are not proper criteria for resolving obviousness. In re Warner, 379 F.2d 1011, 154 USPQ 173 (CCPA 1967).

Because the present application and **Wiser** are so different, it would not have been obvious to one skilled in the art to combine aspects of **Wiser** to aspects of the present application. The present application and **Wiser** perform different functions. The present application and

Wiser have different purposes and operate in vastly different architectures using vastly different methods. **Wiser** is a computer implemented online music distribution system for secure delivery of media files for use on predetermined media players. The present application relates to the creation and use of independent secure cookies between a server and a client.

Objects disclosed in **Wiser** are not the same as objects disclosed in the present application. **Wiser** requires three distinct objects that are essential to **Wiser** in performing its stated goal of secure media delivery and use, whereas the present application may perform its stated goal of enabling the transfer of secure data on a network between a client (singular) and a server using a secure cookie. The three **Wiser** objects are: media content; a media voucher object; and a passport object. See **Wiser**, col. 6, lines 36-47. None of these **Wiser** objects is the same or equivalent to the secure cookies disclosed in the present application.

Wiser's media content (object) is stored in media data files that are encrypted when purchased, using encryption keys of the purchasers, whereas the present application does not require any of its objects to be stored in any other type of file, especially purchased files. Further, the present application does not require the encryption of any shell file. No objects disclosed in the present application are intended to be encapsulated in media files.

Wiser's media voucher object, in the following steps, is created by a content manager, passed to an intermediary server, forwarded to an intermediary web browser, and finally passed to a media player, for whom it is intended. See **Wiser**, col. 8, lines 19-41. The objects disclosed in the present application are created directly by a server and then transmitted directly to their intended client user.

Wiser's passport object is also not created by a server like the objects in the present application. The passport is issued by a licensing center as a prerequisite for any media file transactions. See **Wiser**, col. 8, line 43 – col. 9, line 37. In contrast, in the present application, a server creates objects when and as they are needed when interacting with a client.

Because the rejection of these claims is based upon impermissible hindsight, withdrawal of these rejections is respectfully solicited.

4. The rejection of claims 90 and 91 under 35 U.S.C. § 103(a) are improper because they appear to be based on impermissible hindsight.

Shi discloses the use of multiple cookies to authenticate users. However, each cookie in **Shi** is a single entity. Nowhere in **Shi** does a cookie involve a multitude of secure cookies. Rather, **Shi** uses one cookie at a time. Specifically, **Shi** points out that after the user has been authenticated, a server will send a login HTML form, requesting a user id and password, and a cookie, which includes the URL of the requested document. See **Shi**, col. 8, lines 14-35. After the user successfully logs into the system, the cookie is destroyed and a new one is created. See **Shi**, Fig. 4. Should the login be unsuccessful, a custom error message is generated and the former cookie is destroyed. Id. This method of using new, single entity cookies does not correlate with the present application. The present application incorporates a set of secure cookies, wherein at least one is a seal cookie, into at least one secure cookie. See Specification, §§ 3.2, 4.1, Fig. 4. A seal cookie provides an additional layer of security by providing a method to determine if a cookie has been altered. Id. at § 3.2. Simply, **Shi** does not disclose or suggest any seal cookie or its equivalent. Nowhere does the system in **Shi** checks whether any cookie has been altered.

Because **Shi** does not suggest such combination of secure cookies, claims 90 and 91 appear to be rejected on impermissible hindsight. Withdrawal of this rejection is respectfully requested.

5. The rejection of claims 92, 93 and 109 under 35 U.S.C. § 103(a) are improper because they appear to be based on impermissible hindsight.

As argued previously in section II.B.4., **Shi** does not disclose a seal cookie. It therefore follows that the rejection of claims 92, 93 and 109 are based on impermissible hindsight. **Shi** does check whether the user id and password is properly authenticated. See **Shi**, col. 8, lines 47 – 60. However, this verification method is not the same or equivalent to the verification method of the present application. A completely different method, the integrity check value in the present application concerns the verification of the seal cookie by using the public key of the cookie-issuing server. See Specification, § 3.2.1. If the integrity verification is successful, then no alteration of the cookies has occurred. Id. Furthermore, if the cookies are valid, then the user is permitted to execute transactions based on the values of the cookies. Id. Nowhere in **Shi** is such step imposed.

In addition, **Shi** does not include in its system a signature of a message digest signed by using a private key. What **Shi** discloses is a unique id, which is "a secret handle that is an entry into a table of credentials stored in the database associated with the session manager." See **Shi**, col. 8, lines 54-66. However, unlike the present application, this

unique id does not utilize a message digest signature and a private key to identify the user. Rather, the unique id bears the user's credentials and thus does not require a message digest signature for identification.

Moreover, **Shi**'s unique id does not disclose or implicate the use of encrypting and decrypting via a private key. Rather, **Shi** uses a DCE Security Server for authentication services. Yet, **Shi** does not explain how such method, if at all, encrypts and decrypts information, let alone selected conforming client data. Hence, without this teaching, it could not be obvious that **Shi** exercises a private key for encryption and decryption.

Since the rejection of claims 92, 93 and 109 appear to be based on impermissible hindsight, applicant respectfully requests that the rejection be withdrawn.

6. The rejection of claim 94 under 35 U.S.C. § 103(a) is improper because **Shi** does not teach or suggest all the claimed limitations.

In addition to the arguments made in section II.A.1., **Shi** does not teach a system with secure cookies having at least a name and value pair. As argued in section II.B.1., the prior art reference must teach or suggest all the claim limitations in order to make a prima facie case of obviousness. See MPEP § 2143. Although the examiner correctly says that **Shi** discloses name/value pairs, the obviousness rejection should be overturned because **Shi** still does not teach or suggest the creation or use of a "secure cookie." Without this disclosure, it would not be obvious to one of ordinary skill in the art that at least a name and value pair would be included within the creation or use of a "secure cookie." Moreover, because independent claim 79 has not been rejected as obvious under 35 U.S.C. § 103(a), then any claim depending from it is nonobvious. See In re Fine, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988).

Respectfully, applicant requests that this rejection be withdrawn based upon the foregoing arguments.

7. The rejection of claim 95 under 35 U.S.C. § 103(a) is improper because **Shi** fails to disclose this limitation.

Shi discusses specified domains and paths in searching for valid cookies. See **Shi**, col. 7, lines 21-60. However, nowhere does the description include or suggest the use of a flag. The present application defines "flag" as a thing that "specifies whether or not all machines within a given domain can access the variable in the cookie." See Specification, § 2.1. "If true all servers in the specified Domain_Name can use the cookie (and the browser will supply the cookie to all servers in that

domain). If false Domain.Name is interpreted as a host name, which is the only host to whom the browser will give that cookie." Id. Instead, **Shi** focuses its attention on "tail matching." See **Shi**, col. 7, lines 26-35. This totally different concept refers to the matching of the domain attribute against the tail of host's fully qualified domain name. Id. Exemplifying "tail matching," **Shi** teaches that a domain attribute called "acme.com" would match with host names such as "anvil.acme.com" and "shipping.crate.acme.com." **Shi** would only send cookies if a match is made. In contrast, cookies in the present application will only be sent by the browser if those cookies are relevant to the server by virtue of the Domain_Name and Flag fields. See Specification, § 2.1.

Because neither flag nor its equivalent is disclosed in **Shi**, withdrawal of this claim rejection is requested.

8. The rejection of claims 105-107 and 110 under 35 U.S.C. § 103(a) is improper because it appears to be based on impermissible hindsight.

Shi discloses a method of authentication by use of Distributed Computing Environment (DCE), a known distributed file system. Under DCE, a user first enters a password to obtain a Kerberos ticket to establish his identity, as well as an authentication identifier known as PAG (Process Authentication Group). See **Shi**, col. 5, line 61 – col. 6, line 11. It is known that DCE credentials are encrypted by a secret key unknown to the user but known to the server.

However, the present application does not use a DCE. Even if the examiner argues that the present application uses a DCE-equivalent, at the time **Shi** was issued, there was no such suggestion or motivation to create "secure cookies" as in the present application. Hence, there could not have been any suggestion or motivation to incorporate claims 105-107 and 110.

Moreover, as argued in section II.B.1., since claims 105-107 and 110 are dependent upon the nonobvious independent claim 99, then these claim limitations necessarily becomes nonobvious.

As such, withdrawal of the rejection is respectfully requested.

C. The remaining prior art reference of record do not anticipate the present application.

Applicant would like to thank the examiner for his consideration of United States Patent No. 6,049,877 to White, entitled "Systems, Methods and Computer Program Products for Authorizing Common Gateway Interface Application Requests." However,

applicant asserts that like **Shi**, this patent only discloses conventional cookies and does not disclose secure cookies or any security measures relating to cookies. Therefore, this patent cannot anticipate the present application as disclosed and claimed.

III. Conclusion

For all of the reasons advanced above, Applicant respectfully submits that the application is in condition for allowance and that action is respectfully solicited. If there are any outstanding issues that might be resolved by an interview or an Examiner's amendment, the Examiner is requested to call Applicant's agent at the telephone number shown below.

The Commissioner is hereby authorized to charge any additional fees, which may be required, or credit any overpayment, to Deposit Account No. 501450.

In the event that an extension of time is required, or may be required in addition to that requested in a petition for an extension for time, the Commissioner is requested to grant a petition for that extension of time which is required to make this response timely and is hereby authorized to charge any fee for such an extension of time or credit any overpayment for an extension of time to Deposit Account No. 501450.

Respectfully submitted,

David G. Grossman
Registration No. 42,609

Date: XXX. XX, 2004

George Mason University
Office of Technology Transfer, MSN 5G5
4400 University Drive
Fairfax, VA 22030
(703) 338-6333